UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/062,621	01/31/2002	John A. Copeland III	10775-36791	2472

7590 09/29/2005

John R. Harris
Morris, Manning & Martin, LLP
1600 Atlanta Financial Center
3343 Peachtree Rd., N.E.
Atlanta, GA 30326

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 09/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	10/062,621	COPELAND, JOHN A.
	Examiner	Art Unit
	Ronald Baum	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *09082005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1- 22 are pending for examination.

2. Claims 1- 22 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1,4,9,10,14,17 and 20 are rejected under 35 U.S.C. 102(b) as being anticipated by Shipley, U.S. Patent 6,119,236.

4. As per claim 1; "A method for determining unauthorized network usage, comprising the steps of:

capturing packet header information from communications on a network;

determining valid connections or data flows [col. 3,lines 17-col. 12,line 35, whereas the "... dynamically detect patterns of behavior ...", "... automatically determining the configuration of the LAN...", etc., clearly encompasses the claimed limitations, insofar as for the determining /detection /comparison /control of the firewall to occur, the packet flow clearly must be collected per se, and such collection involves collection of the packets header data (i.e., the IP address, port, status flags, etc.,), as broadly interpreted by the examiner.];

determining hosts on the network that act as a client and server for each valid connection or data flow [col. 3,lines 17-col. 12,line 35, whereas the LAN and network aspects of the INSD

interfaced to said network of multiple nodes, and the Internet /LAN port aspects insofar as port identification as relates to the Internet deals with port to port service designation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and

determining network services being used by every host in a predefined group of hosts [col. 3,lines 17-col. 12,line 35, whereas the LAN and network aspects of the INSD interfaced to said network of multiple nodes, and the Internet /LAN port aspects insofar as port identification as relates to the Internet deals with port to port service designation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.].".

5. Claim 4 ***additionally recites*** the limitation that; "The method of claim 1, further comprising the steps of:

storing an allowed network services profile;

comparing allowed network services with observed network services; and

generating an alarm when an observed network service is not an allowed network service.".

The teachings of Shipley suggest such limitations (col. 3,lines 17-col. 12,line 35, whereas the "... assign weight to breach...", and "... react operation ..." aspects of the post "... look for known patterns ...", that involve the control and notification (i.e., alarm) of the network associated firewall /gateway node, subsequent to a storing of packets (clearly associated with the services defined by the port access IP addressing/service request) to be compared to a predefined profile (that itself is stored in the node at some level), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

6. As per claim 9; "A method for determining unauthorized network usage, comprising the steps of:

capturing packet header information from communications on a network;

determining hosts on the network that act as a client and server for each valid connection or data flow;

determining network services being used by every host in a predefined group of hosts [col. 3,lines 17-col. 12,line 35, whereas the LAN and network aspects of the INSD interfaced to said network of multiple nodes, and the Internet /LAN port aspects insofar as port identification as relates to the Internet deals with port to port service designation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and

generating an alarm upon an observed network service not being included in an, allowed network service profile [col. 3,lines 17-col. 12,line 35, whereas the "... assign weight to breach...", and "... react operation ..." aspects of the post "... look for known patterns ...", that involve the control and notification (i.e., alarm) of the network associated firewall /gateway node, subsequent to a storing of packets (clearly associated with the services defined by the port access IP addressing/service request) to be compared to a predefined profile (that itself is stored in the node at some level), clearly encompasses the claimed limitations as broadly interpreted by the examiner.].".

As per claim 17, this claim is the apparatus/system for the method claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection; "A system for determining unauthorized network usage, comprising:

a monitoring device operable to observe communication packets on a network;

a computer system operable to capture packet header information from observed communication packets;

the computer system operable to determine valid connections or data flows;

the computer system operable to determine hosts on the network that act as a client and server for each valid connection or data flow; and

the computer system operable to determine network services being used; and

the computer system operable to generate an alarm when an observed network service is not an allowed network service.".

7. As per claim 10; "A method for determining unauthorized network usage, comprising the steps of:

capturing packet header information from communications on a network;

determining valid connections or data flows [col. 3,lines 17-col. 12,line 35, whereas the "... dynamically detect patterns of behavior ...", "... automatically determining the configuration of the LAN...", etc., clearly encompasses the claimed limitations, insofar as for the determining /detection /comparison /control of the firewall to occur, the packet flow clearly must be collected per se, and such collection involves collection of the packets header data (i.e., the IP address, port, status flags, etc.,), as broadly interpreted by the examiner.];

storing an allowed network service port profile for each in a predefined host group;

determining observed network service port numbers being used by every host in the predefined host group for each valid connection or data flow [col. 3,lines 17-col. 12,line 35, whereas the LAN and network aspects of the INSD interfaced to said network of multiple nodes, and the Internet /LAN port aspects insofar as port identification as relates to the Internet deals with port to port service designation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

comparing the allowed network service port profile with observed network service port numbers; and

generating an alarm when an the observed network service port number is not included in the allowed network service port profile [col. 3,lines 17-col. 12,line 35, whereas the "... assign weight to breach...", and "... react operation ..." aspects of the post "... look for known patterns ...", that involve the control and notification (i.e., alarm) of the network associated firewall /gateway node, subsequent to a storing of packets (clearly associated with the services defined by the port access IP addressing/service request) to be compared to a predefined profile (that itself is stored in the node at some level), clearly encompasses the claimed limitations as broadly interpreted by the examiner.].".

8. Claim 14 ***additionally recites*** the limitation that; "The method of claim 10, further comprising the step of

building the network service port profile based upon the observed network service ports observed during a profile generation time period.".

The teachings of Shipley suggest such limitations (col. 3,lines 17-col. 12,line 35, whereas the "... assign weight to breach...", and "... react operation ..." aspects of the post "... look for known patterns ...", that involve the control and notification of the network associated firewall, subsequent to a storing of packets (clearly associated with the services defined by the port access IP addressing/service request) to be compared to a predefined profile (that itself is stored in the node at some level), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

9. Claim 20 ***additionally recites*** the limitation that; "The system of claim 17, further comprising

the computer system operable to build a network service profile based upon network services observed during a profile generation time period.".

The teachings of Shipley suggest such limitations (col. 3,lines 17-col. 12,line 35, whereas the "... assign weight to breach...", and "... react operation ..." aspects of the post "... look for known patterns ...", that involve the control and notification of the network associated firewall, subsequent to a storing of packets (clearly associated with the services defined by the port access IP addressing/service request) to be compared to a predefined profile (that itself is stored in the node at some level), clearly encompasses the claimed limitations as broadly interpreted by the examiner.).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2,3,5 and 6-8 and 11-13,15,16 and 18,19,21,22 rejected under 35 U.S.C. 103(a) as being unpatentable over Shipley, U.S. Patent 6,119,236 as applied to claims 1,4,10,17, respectively, above, and further in view of Vaid et al, U.S. Patent 6,502,131 B1.

10. Claim 2 ***additionally recites*** the limitation that; "The method of claim 1, further comprising the step of

displaying indicia indicating observed network services during a monitoring period.".

11. Claim 3 ***additionally recites*** the limitation that; "The method of claim 2, further comprising the step of

displaying an indication of the observed network services which were previously seen during the presentment period.".

12. Claim 5 ***additionally recites*** the limitation that; "The method of claim 3, further comprising the step of

displaying indicia indicating whether the observed network services is not an allowed network service.".

13. Claim 6 ***additionally recites*** the limitation that; "The method of claim 4, further comprising the step of

building a network service profile based upon network services observed during a profile generation time period.".

14. Claim 7 ***additionally recites*** the limitation that; "The method of claim 4, further comprising

editing the allowed network services profile.".

15. Claim 8 ***additionally recites*** the limitation that; "The method of claim 4, further comprising the step of

editing the allowed network services profile for a block of network address.".

16. Claim 11 ***additionally recites*** the limitation that; "The method of claim 10, further comprising the step of

displaying indicia indicating the observed network service port numbers during a present monitoring period.".

17. Claim 12 ***additionally recites*** the limitation that; "The method of claim 11, further comprising the step of

displaying an indication of the observed network service port numbers which were previously seen during the presentment period.".

18. Claim 13 ***additionally recites*** the limitation that; "The method of claim 12, further comprising the step of

displaying indicia indicating whether the observed network service port numbers is included in the allowed network service port profile.".

19. Claim 15 ***additionally recites*** the limitation that; "The method of claim 10, further comprising

editing the allowed network service port profile.".

20. Claim 16 ***additionally recites*** the limitation that; "The method of claim 15, further comprising the step of

editing the allowed network service port profile for a block of network addresses.".

21. Claim 18 ***additionally recites*** the limitation that; "The system of claim 17, further comprising

a monitor coupled to the computer system operable to display indicia indicating observed network services during a monitoring period.".

22. Claim 19 ***additionally recites*** the limitation that; "The system of claim 18, further comprising

the monitor operable to display indicia indicating whether the observed network services is not an allowed network service.".

23. Claim 21 ***additionally recites*** the limitation that; "The system of claim 17, further comprising

an editor couple to the computer system operable to edit the allowed network services profile.".

24. Claim 22 ***additionally recites*** the limitation that; "The system of claim 21, further comprising

the editor operable to edit the allowed network services profile for a block of network address.".

The teachings of Shipley suggest the base claims limitations (see "As per claim 1, ... As per claim 4, ...10, ...17" paragraphs above) *without explicitly teaching* of the use of "... displaying indicia ... observed network services ... monitoring period ...", "... displaying indicia ... observed network services ... presentment period ...", "... displaying indicia ... observed network services ... not an allowed ... service ...", "...building [and] editing a network service [and block of network address] profile ... observed ... profile generation time ...", and, "... displaying [and editing associated profile] indicia ... observed network service port ... present monitoring period [and included] ...", as a response/react/alarm interface functionality.

Vaid et al, teaches of using/displaying indicia dealing with the various aspects of network traffic management, and associated setup of display criteria and displaying thereof, indicating traffic/traffic flow via the packet level/port/IP address objects rendered on said display/terminal device, implemented using various object oriented/GUI (see figures 1-19 and associated descriptions). The Vaid et al invention also clearly encompasses the security aspects associated with the applicants network communications monitoring aspects insofar as it is inherent that in the process of quality of service monitoring per se, the loss of packets, bandwidth/latency aspects of traffic flow, and traffic profiles in of themselves deal with the security aspects of denial of service, and intrusion detection (i.e., denial of unauthorized access to a network through a gateway such as a firewall); clearly security aspects associated with the applicants claimed invention.

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Shipley network security device and method for firewall control via packet flow monitoring/control, with the Vaid et al teachings of actual firewall/network gateway node directory enabled policy management tool for intelligent traffic management, in order to provide the firewall configuration and efficient control thereof, upon the Shipley network resulting control of said firewall.

Such motivation to combine would clearly encompass the need to allow comprehensive firewall configuration and efficient control in an intrusion detection/packet scanning environment for the network communications (i.e., Vaid et al col. 2,lines 46-col. 4,line 13).

Conclusion

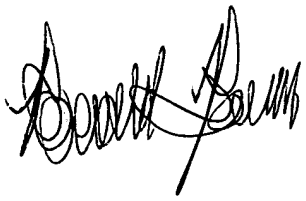
25. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

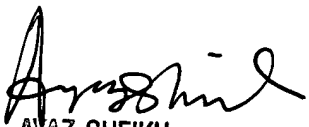
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner





AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100